REMARKS

Deficiencies in the Final Office Action

Applicants respectfully submit that the Final Office Action (dated September 11, 2008) is not proper because of fundamental deficiencies therein. Applicants respectfully direct the Examiner's attention to the Final Office Action, pp. 5-6. In particular, the Applicants note that the Examiner has failed to establish a prima facie case of obviousness because the Examiner has failed to address the last claim element of claim 3. Applicants request the Examiner to either allow claim 3 or, at a minimum, withdraw the finality of the Office Action in light of the deficiency.

Status of Claims

Claims 1-3, 6 and 28-29 have been amended to address informalities raised by the Examiner. Claims 9-27 are cancelled. Claims 31-33 have been added. Claims 1-8 and 28-33 are pending and presented for examination.

Information Disclosure Statement

Applicants acknowledge and appreciate that the Information Disclosure Statement submitted on July 7, 2008, has been acknowledged and is being considered by the Examiner.

Claims Objections

The Examiner objected to claims 1, 2, 6, 9, 28 and 29 due to informalities. Applicants maintain that the claims, as previously written, are allowable and in compliance with the definiteness requirement of 35 U.S.C. §112. In the interest of expediting prosecution, Applicants have amended claims 1, 2, 6, 9, 28 and 29 replacing "capable of" with "adapted to." These amendments obviate the Examiner's rejection.

Claims Rejections

The Examiner rejected claims 1-8 and 28-30 under 35 U.S.C. 103(a) as being anticipated by US Publication 2004/0139322A1 ***(Kaler)*** in view of US Publication 2004/0139352 ***(Shewchuk)***. Applicants respectfully traverse this rejection.

For ease of discussion, claim 6 is discussed first. Claim 6, depending from method claim 1, calls for determining an alternative intermediate device along a different transmission path that is adapted to provide the level of security represented in response to determining that the adjacent intermediate device in the transmission path is not adapted to provide the level of security. By allowing alternate devices to be sought out if adjacent devices are not able to provide the desired security, a secure transmission path may be found at the desired security level, for example.

The Examiner's rejection of claim 6 is not sustainable because ***Kaler*** and ***Shewchuk***, either alone or in combination, do not teach or suggest all of the claimed features. For example, as admitted by the Examiner, ***Kaler*** does not teach the claimed feature of determining an alternative intermediate device along a different transmission path that is adapted to provide the level of security represented in response to determining that the adjacent intermediate device in the transmission path is not adapted to provide the level of security. *See* Office Action, p.7. The Examiner attempts to apply ***Shewchuk*** to teach this claimed feature. *See id.* ***Shewchuk***, however, fails to teach the claimed feature, as called for in claim 6.

Shewchuk teaches that a requesting client 511 first communicates with a validating message processor 531 to establish an encapsulated security token. *See* ***Shewchuk***, ¶¶[0115]-[0116] and Fig. 5. Once the security token is established, the client then sends the encapsulated security token to a server message processor 521 in order to create a secure relationship. *Id.* In

other words, the client must first go to a first server in order to encapsulate its token, then the client goes to a second server to establish a trusted relationship. As such, ***Shewchuk*** does not teach an alternative intermediate device on a different transmission path is chosen in response to determining that the adjacent intermediate device is not capable of providing the level of security. ***Shewchuk*** does not teach the claimed feature because going to a first server then to a second server *is* the desired path taught. Likewise, because it is the desired path taken, there cannot be an alternative device or a different path chosen. Furthermore, an inspection of ***Shewchuk***, Fig. 5 reveals that there are no intermediate devices on any transmission paths between the requesting client 511 and either of the validating message processor 531 or the server message processor 521. In fact, Fig. 5 shows direct connections between the requesting client and both the validating message processor and the server message processor. As such, ***Shewchuk*** cannot teach an **alternative intermediate device** on a different transmission path, as called for in claim 6.

Kaler fails to remedy the fundamental deficiencies of ***Shewchuk***. For at least the above mentioned reasons, it is respectfully submitted that claim 6 is allowable.

Claim 3 is discussed next. Claim 3, a method depending from claim 1, calls for, among other things, transmitting to the adjacent intermediate device in the transmission path information representative of the level of security that is desired in order to prompt the adjacent intermediate device in the transmission path to execute at least one module that allows the adjacent intermediate device in the transmission path to provide the level of security. ***Kaler*** fails to teach this feature for the following reasons, and additionally, for the reasons cited below with respect to claim 1. The Examiner argues that this feature is taught by ***Kaler*** in ¶[0086]. *See* Office Action, p.12. Specifically, the Examiner points to the teaching of ***Kaler*** describing

functional result-oriented step for exchanging information. *See* ***Kaler,*** ¶[0086]. This paragraph in ***Kaler*** teaches that "any corresponding acts for accomplishing the result of exchanging information." *Id.* Fig. 3 in ***Kaler***, and the surrounding context of ¶[0086], make it clear that "information" refers to "context information. *See* ***Kaler***, Fig. 3. Thus, this reference does not teach or suggest the claimed feature of transmitting to the adjacent intermediate device in the transmission path information representative of the level of security that is desired in order to prompt the adjacent intermediate device in the transmission path to execute at least one module that allows the adjacent intermediate device in the transmission path to provide the level of security does not call for an exchange of context information. The "corresponding acts" referred to by the Examiner do not involve prompting the adjacent intermediate device in the transmission path to execute at least one module that allows the adjacent intermediate device in the transmission path to provide the level of security, as called for in claim 3. *See* ***Kaler***, ¶[0083].

Claim 3 also calls for comparing the adjacent intermediate device in the transmission path to a list of trusted devices in the header portion of the object. The Examiner cites ***Kaler***, ¶¶[0016], [0030], [0081] & [0110], as teaching this feature, but the cited references are, in fact, silent regarding this feature. The Examiner generally cites to several paragraphs from ***Kaler***, but fails to identify where specifically the claimed features are disclosed in this reference. For this reason, the Applicants respectfully request the Examiner to **specifically identify** where ***Kaler*** discloses (1) comparing the adjacent intermediate device in the transmission path to (2) the list of trusted devices, (3) where the list is in the header portion of (4) the object.

For at least the aforementioned reasons, claim 3 and its dependent claims are allowable.

Claim 1 is discussed next. Claim 1, directed to a method, calls for (1) determining security information associated with at least one object of a transaction, wherein the object is to

be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device.

The ***Kaler*** reference, in contrast to the Examiner's assertion, does not teach the claimed feature of determining if an adjacent intermediate device in the transmission path is adapted to provide a level of security indicated by at least a portion of the security information. In particular, as stated by the Examiner on page 4 of the Office Action, a first and second end message processor establish a secure context with each other. *See* ***Kaler***, ¶[0019]. Thus, ***Kaler*** teaches establishing a secure context between endpoints of a transmission (*i.e.,* the source and target, as taught in claim 1). ***Kaler***, however, is not concerned with intermediate (intervening) devices in the transmission path (*e.g.,* network routers, as an illustrative example). The security measures in ***Kaler*** are implemented in the application layer during the transmission (*i.e.,* not at lower level layers involved in transport such as the transport layer, the network layer, the data link layer or the physical layer). *See, e.g.,* ***Kaler***, ¶[0016], ¶[0020] and Abstract. Transmission path devices, such as network routers, as an example, handle data at lower levels, not upper levels such as the application layer. By using the application layer security scheme, intermediate (intervening) devices in a transmission path in ***Kaler*** would not be handling any secure data in a transmitted packet. Therefore, by ***Kaler's*** teaching, there is no reason to check security levels at an intermediate (intervening) device, and in fact, ***Kaler*** does not disclose such a teaching. *See, e.g.,* ***Kaler***, Fig. 2 and ¶[0020]. Fig. 2 in ***Kaler*** specifically shows a secure context between endpoints wherein the security level of Intermediary Message Processors 206 & 207 is ignored. *See* ***Kaler***, Fig. 2. As such, ***Kaler*** cannot, and does not, teach determining if an adjacent intermediate remote device in the transmission path is adapted to provide a level of security

indicated by at least a portion of the security information, as taught in claim 1 of the instant Application.

With respect to Fig. 6 in ***Kaler***, to the extent it is the Examiner's position that this figure teaches the claimed feature of determining security information associated with at least one object of a transaction, the Examiner's position is not correct. Fig. 6 shows a client 601 has established a secure context with an intermediate device 605. Fig. 6 also shows that a server 602 has established a separate secure context with the intermediate device 605. Because of the separate contexts, ***Kaler*** teaches that the client and server do not trust each others' content. Fig. 6, however, does not teach determining security information associated with at least one object, as called for in claim 1. Fig. 6, and accompanying text, is silent with respect to objects. *See* ***Kaler***, Fig. 6 & ¶¶[0012]-[0013]. As such, the intermediate device in ***Kaler***, Fig. 6, as argued by the Examiner, does not teach determining security information associated with at least one object feature of claim 1.

It is respectfully submitted that ***Kaler*** actually *teaches away* from the claimed feature because, as noted above and in the ***Kaler*** reference, intervening devices along a transmission path are ignored for security purposes. As such, the subject matter of the instant Application and the teachings of ***Kaler*** are incompatible.

For at least the aforementioned reasons, claim 1 and its dependent claims are allowable. For similar reasons, claim 28 and its dependent claims are also allowable.

Applicants respectfully assert that ***Kaler***, ***Shewchuk***, and/or their combination do not teach or disclose all of the elements of the claims the present invention. In making an obviousness rejection, it is necessary for the Examiner to identify the reason why a person of ordinary skill in the art would have combined the prior art references in the manner set forth in

the claims. *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1741 (2007). Applicants respectfully submit that the Examiner has not met this burden. If in fact, as illustrated below, ***Kaler*** and ***Shewchuk*** are incompatible, and consequently those skilled in art would not combine them and make all of the elements of claims of the present invention obvious. ***Kaler*** and ***Shewchuk*** are directed toward two very different methods of establishing security. ***Kaler*** describes establishing a secure context between endpoints, and ***Shewchuk*** teaches client server trust relationships using security token protocols. One skilled in the art would not combine and endpoint based methodology with a server/token based methodology because endpoint-to-endpoint security is designed such that interaction with a server is not necessary. The endpoints may communicate directly with each other and establish a secure context independently over a network. Accordingly, Applicants respectfully submit that a *prima facie* case of obviousness has not been established in rejecting claims 1-8 and 28-30.

Applicants respectfully assert that in light of the amendments and arguments provided throughout the prosecution of the present application, all claims of the present application are now allowable and, therefore, request that a Notice of Allowance be issued. Reconsideration of the present application is respectfully requested.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is respectfully requested to call the undersigned attorney at the Houston, Texas telephone number (713) 934-4064 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 23720

Date: November 11, 2008

By: /Ruben S. Bains/
Ruben S. Bains, Reg. No. 46,532
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4064
(713) 934-7011 (facsimile)
ATTORNEY FOR APPLICANT(S)